REMARKS

As stated above, Applicants appreciate the Examiner's thorough examination of the subject application and request reexamination and reconsideration of the subject application in view of the preceding amendments and the following remarks. Applicants have carefully reviewed and considered the Office Action mailed on 29 November 2005. Reconsideration and allowance of the subject application, as amended, are respectfully requested.

Claims 24, 29, 34 and 39 are amended; as a result, claims 24-43 are now pending in this application.

Regarding Items 1-2 of the subject action, the Examiner provides a response to the Request for Continued Examination filed 12 September 2005. In the response the Examiner appears to suggest that the limitation "via a network infrastructure" is interpreted as "using/over a network". The Examiner also appears to suggest that the "via a network infrastructure" limitation is not supported in the specification of the application.

As described below, independent claims 24, 29, 34 and 39 have been amended to address this issue.

Regarding Items 3 and 4 of the subject action, the Examiner rejected claims 24-43 under 35 USC § 112, first paragraph, as failing to comply with the written description requirement. In particular, the Examiner appears to state the specification of the application does not disclose that a security association (SA) is transferred from an IHA to a network adapter via a network infrastructure.

Independent claims 24, 29, 34 and 39 have been amended to remove the phrase "and provided to said network adapter via a network infrastructure". The Applicants respectfully disagree with the Examiner's assertion and believe support is provided for this feature in the specification of the application. However, to facilitate prosecution of this application the feature has been removed.

Regarding Items 5-6, the Examiner rejects claims 24-43, under 35 USC §103(a), as being unpatentable over Anand et al. (U.S. Patent No. 6,370,599; hereinafter Anand) in view of Yoshida (U.S. Patent No. 5,928,372; hereinafter Yoshida).

The Examiner points to Anand as disclosing a system comprising: a network adapter being capable of being coupled to an information handling apparatus (IHA) via a bus (fig.1, elements 53, 21-23). The Examiner also points to Anand as disclosing that the network adapter comprising an integrated circuit capable of receiving a security association (SA) generated by said IHA (col. 8, lines 21-35, figures 3-4 and corresponding text). The Examiner also points to Anand as disclosing transferring data from the IHA (i.e., the CPU) to the network adapter.

The Examiner concedes that Anand does not disclose verification of data transferred between the CPU and the network adapter, which is a peripheral device. The Examiner points to Yoshida as disclosing data verification in a data transfer system in which a host processor transfers data and a first integrity indicator generated by the host processor to a peripheral device (i.e., the hard disk unit) and the peripheral device generates a second integrity indicator, verifies that the received data is similar to the data sent by the host processor by comparing said first integrity indicator to said second integrity indicator (col. 1, line 60 to col. 2, line 20, figures 20-21 and corresponding text). The Examiner is understood to claim that Anand and Yoshida are analogous art because they are from a similar problem solving area, which is transferring data from a host processor to a peripheral device. The Examiner goes on to suggest that it would have been obvious to one or ordinary skill in the art at the time of the invention was made to incorporate the Yoshida's teaching of data verification into the Anand system in order to insure the correctness of the reception data (col. 9, lines 47-54).

Applicants claim (in currently amended independent claim 24):

24. A method, comprising: receiving, by a network adapter, a security association and a first integrity indicator, said SA and first integrity indicator being generated by an information handling apparatus (IHA); generating, by said network adapter, a second integrity indicator based on said SA; verifying, by said network adapter, that said SA within said network adapter is substantially similar and the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator; and <u>using said SA to encode data for transmitting to a network infrastructure device</u>.

Applicants claim (in currently amended independent claim 29):

29. An apparatus comprising: a network adapter comprising an integrated circuit, said integrated circuit is capable of receiving a security association (SA) and a first integrity indicator, said SA and first integrity indicator being generated by an information handling apparatus (IHA), said integrated circuit being further capable of generating a second integrity indicator based on said SA, said integrated circuit being further capable of verifying that said SA received by said integrated circuit is substantially similar the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator, said integrated circuit being further capable of using said SA to encode data for transmitting to a network infrastructure device.

Applicants claim (in currently amended independent claim 34):

34. An article comprising: a storage medium storing instructions that when executed by a machine result in the following operations: receiving, by a network adapter, a security association (SA) and a first integrity indicator, said SA and first integrity indicator being generated by an information handling apparatus (IHA); generating, by said network adapter, a second integrity indicator based on said SA; verifying, by said network adapter, that said SA within said network adapter is substantially similar the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator; and using said SA to encode data for transmitting to a network infrastructure device.

Applicants claim (in currently amended independent claim 39):

39. A system, comprising: at least one network adapter being capable of being coupled to an information handling apparatus (IHA) via a bus, said

network adapter comprising an integrated circuit capable of receiving a security association (SA) and a first integrity indicator, said SA and first integrity indicator being generated by said IHA, said integrated circuit being further capable of generating a second integrity indicator based on said SA, said integrated circuit is substantially similar the SA generated by said IHA by comparing said first integrity indicator to said second integrity indicator, said integrated circuit being further capable of using said SA to encode data for transmitting to a network infrastructure device.

The above identified application provides support for the subject matter amended to independent claims 24, 29, 34 and 39. In particular, regarding a security association (SA) being used to encode data for transmission, the subject application cites:

> Checker 28 may also transfer security association 32' to encoder/decoder 31 to enable the encoding of data from IHA 12 before the data is transmitted onto network media 14, and to enable the decoding of data packets from network media 14 before data within such packets are transferred to IHA 12. Encoder/Decoder 31 using known decoding techniques may decode the data packets. Memory controller 24 may transfer data from the decoded data into memory 38. (page 8, end of first paragraph) (emphasis added)

In regards to transferring data to a network infrastructure device, the above identified application cites:

> Adapter 20 transfers and receives information or data in packet form to and from IHA 19 within node 9 via network media 14 and network infrastructure device 16. As with IHA 12, IHA 19 may comprise, without limitation, any device, machine, computer or processor that handles, routes, or processes information or data. Network infrastructure device 16 may comprise an apparatus for routing, switching, repeating or passing information or data via a network such as a router, server, switch, or hub, for example. Network media 14, the medium in which data is transferred, comprises, but is not limited to, wires, optical fiber

> cables, or radio waves." (page 5, last paragraph to top of page 6) (emphasis added)

Applicants respectfully assert that the combination of the teachings of Anand and Yoshida fails, at least, to disclose or suggest the underlined portions of Applicants' amended independent claims 24, 29, 34 and 39, namely "using said SA to encode data for transmitting to a network infrastructure device". Accordingly, Applicants respectfully assert that the combination of the teachings of Anand and Yoshida is not a proper basis for a 35 USC §103(a) rejection, as the combination of the teachings of Anand and Yoshia fails to disclose each and every element of the Applicants' claimed invention.

Returning to the subject action, the Examiner states that:

> Yoshida teaches data verification in a data transfer system in which a host processor transfers data and a first integrity indicator generated by the host processor to a peripheral device (i.e., the hard disk unit) and the peripheral device generates a second integrity indicator, verifies that the received data is similar to the data sent by the host processor by comparing said first integrity indicator to said second integrity indicator (col. 1, line 60 – col. 2, line 20; figures 20-21 and corresponding text). (Page 5 of subject action)

Concerning the passage of Yoshida relied upon by the Examiner, the passage discloses:

> A transfer data verification method in the data processing equipped with an external recording unit according to the present invention for accomplishing the object described above is a method of verifying transferred data in a data processor which incorporates a main board having a microprocessor mounted thereto and an external recording unit for storing data, and wherein the data transfer is effected between the main board and the external recording unit through a specific interface, and this method comprises a first stage in which, when the data transfer is effected between the data processor and the external recording unit, a data check code having a one-byte width is calculated on the data processor side by a predetermined calculation formula by regarding this

> transfer data as serial data; a second stage in which, when the data transfer is effected between the data processor and the external recording unit, a data check code having a one-byte width is calculated on the side of the external recording unit by the same predetermined calculation formula as that of the data processor side on the side of the external recording unit by regarding the transfer data as serial data; a third stage in which, after the data transfer is completely finished, the data check code calculated on the side of the data processor is compared with the data check code calculated on the side of the external recording unit; and a fourth stage in which, when these two data check codes coincide with each other, the data transfer is judged as being effected without error, and when they do not coincide, the data transfer is judged as not being effected normally. (col. 1, line 60 – col. 2, line 20) (emphasis added)

Yoshida is understood to describe a system that verifies the integrity of data transferred between a "main board" and an "external recording unit". Accordingly, Yoshida fails to teach using a security association (SA) to encode data for transmitting to a network infrastructure device.

Further, while the Examiner asserts that "Anand and Yoshida are analogous art because they are from a similar problem solving area, which is transferring data from a host processor to a peripheral device", Applicants respectfully disagree with this assertion.

Upon review, Yoshida is understood to concern data transfers between a computer motherboard and an internal hard disk drive. Accordingly, the data transfer events that are handled by the Yoshida system are comparatively secure, as the data doesn't leave the sanctity of the computer system. However, the data transfer events that are handled by the Applicants' system are substantially more prone to attack / corruption, as the data being prepares (e.g., encoded) for transmission through a network to a network infrastructure device (e.g., network switch, network router, etc.). Accordingly, Applicants respectfully assert that Anand and Yoshida are not analogous art, as the security / corruption risks associated with providing data between a motherboard and a hard disk drive (as apparently described in Yoshida) are quite

different than those associated with preparing and transferring data through a network to a network infrastructure device.

Accordingly, the Applicants respectfully assert that the combination of Anand and Yoshida is not a proper basis for a 35 USC §103(a) rejection, as the combination of the references fails to disclose each and every element of the Applicants' currently amended independent claims 24, 29, 34 and 39. Therefore, the Applicants respectfully assert that amended independent claims 24, 29, 34 and 39 are patentable over the combination of cited references.

As dependent claims 25-28 depend (either directly or indirectly) upon amended independent claim 24, Applicants respectfully assert that claims 25-28 are also patentable over the combination of cited references. Further, as dependent claims 30-33 depend (either directly or indirectly) upon amended independent claim 29, Applicants respectfully assert that claims 30-33 are also patentable over the combination of cited references. Additionally, as dependent claims 35-38 depend (either directly or indirectly) upon amended independent claim 34, Applicants respectfully assert that claims 35-38 are also patentable over the combination of cited references. Finally, as dependent claims 40-43 depend (either directly or indirectly) upon amended independent claim 39, Applicants respectfully assert that claims 40-43 are also patentable over the combination of cited references.

No new matter has been added by these amendments. The Applicants respectfully submit that the claims are in condition for allowance and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicants' attorney (603-668-6560) to facilitate prosecution of this application.

Respectfully submitted,

AVRAHAM MUALEM ET AL.

By their Representatives,

Customer Number: 45459

603-668-6560

Date 2/28/06

By _____
Edmund P. Pfleger
Reg. No. 41,252

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Commissioner of Patents, P.O.Box 1450, Alexandria, VA 22313-1450, on this 28 day of 2006. February .

KYRSTIN RYAN
Name

Kyrstin Ryan
Signature